Department of Justice

Federal Bureau of Investigation

NATIONAL INSTANT CRIMINAL BACKGROUND ELECTRONIC CHECK SYSTEM (NICS E-CHECK)

SECURITY FEATURES USER'S GUIDE

January 10, 2003

Prepared By:

Federal Bureau of Investigation
Criminal Justice Information Services Division
1000 Custer Hollow Road
Clarksburg, WV 26306-0001

TABLE OF CONTENTS

1 INTRODUCTION

The National Instant Criminal Background Check System (NICS) Electronic Check (E-Check) System is designed to allow Federal Firearm Licensees (FFLs) to electronically access, via the Internet, the National Instant Criminal Background Check System in accordance with the Brady Handgun Violence Prevention Act of 1993 (Brady Act).

Currently NICS checks are initiated by FFLs via the telephone. The FFL contacts a NICS Customer Service Representative (CSR). The CSR validates the FFL by obtaining the FFLs license number and an assigned codeword. Once validation is complete, the FFL transmits information supplied by the firearm purchaser on the Bureau of Alcohol, Tobacco, and Firearms (ATF) Form 4473. The CSR enters the information transmitted by the FFL into a computer and initiates the background check. All employees of the FFL use the same codeword when contacting NICS via the telephone.

The FBI NICS E-Check system is designed to provide the FFLs with an alternative means to initiate a NICS background check. The alternative means provided by the system will be through secure Internet access. To use the FBI NICS E-Check system, each employee of the FFL requiring FBI NICS E-Check system access will be required to obtain a digital identifier, called a digital certificate, from the FBI. The digital certificate becomes the personal identifier for each user and is required to access the FBI NICS E-Check system through a Web browser interface via the Internet.

In addition to authentication (identification) of the FFL employee, the digital certificate will provide a means of protection of the information submitted by the FFL from the ATF Form 4473. This information, transmitted over the Internet, is encrypted to prevent unauthorized disclosure or modification.

The purpose of this document is to describe the security protection mechanisms associated with digital certificates, and to provide detailed procedures on how to use these mechanisms to access the FBI NICS E-Check system.

2 SYSTEM SECURITY OVERVIEW

This section describes the end-user security features in use on FBI NICS E-Check.

2.1 System Protection Philosophy

The FBI NICS E-Check system will deny access to any individual whose identification is not known and who has not been approved for access privileges. Identification is established using digital certificates issued by the FBI. A digital certificate is a computer-based record that identifies an individual in an electronic transaction. Just like a driver's license or passport identifies a person in a face-to-face transaction, a digital certificate represents the identity of the person to the FBI for all FBI NICS E-Check web site activities. **Each individual who requires access to FBI NICS E-Check must request and obtain a separate digital certificate. Only one digital certificate will be issued to an individual.**

When a request is made for a digital certificate, the Web browser automatically generates a "key pair". A key pair consists of two mathematically related numbers called the "private" and "public" keys. The public key along with the submitted personal information in the digital certificate request composes the digital certificate. The associated private key remains in the user's browser. The digital certificate cannot be used unless the browser also contains the private key that is related to the public key contained in the digital certificate. In other words, a digital certificate can only be used if the user posses the private key associated with that digital certificate. The private key must be protected in the same manner in which other vital identifying information is protected.

2.2 Protecting Your Private Key

Protection of the private key associated with your digital certificate is accomplished using passwords in your Web browser. Netscape uses a password protected personal "Profile" for each user. All user information including digital certificate(s) is kept separate and protected with a password. This works well in an environment where multiple users share a computer. Each user should create a Netscape profile and protect it with a password prior to requesting a digital certificate using Netscape. (See Section 6.2.1)

Protecting the private key associated with your digital certificate in Netscape is accomplished through the creation of a password protected user profile for each user prior to that user requesting a digital certificate. Private key protection using Internet Explorer is accomplished by password protecting each individual user's digital certificate after it has been downloaded. Specific procedures on how to acquire and protect digital certificates using both Netscape and Internet Explorer browsers can be found in Section 6 of this document.

2.3 FBI NICS E-Check Username

Every FBI NICS E-Check user will chose (or have assigned to them) a 6 to 10 character (letters, numbers or both) unique username. This username provides additional authentication or identification when logging into the FBI NICS E-Check system.

2.4 Digital Certificate Validity Period

To further enhance the security of issued digital certificates, each digital certificate has an imposed expiration date making it useful for a specified period of time. This time period is known as the digital certificate validity period and will range from 1 year to 18 months. Once a digital certificate has expired, it can no longer be used to obtain FBI NICS E-Check access. To replace an expired digital certificate, a new online digital certificate request must be submitted.

2.5 Security Monitoring

All functions performed at the FBI NICS E-Check web site will be monitored 24 hours a day, 7 days a week for misuse and unauthorized access.

3 GETTING HELP

FBI NICS E-Check offers online help by accessing the http://www.nicsezcheckfbi.gov/ Web site then clicking on HELP.

User telephone support can be obtained immediately by dialing the NICS Operations Center toll free at: **1-877-444-6427**.

Telecommunications Device for the Deaf (TDD).

1-877-NICS-TTY (1-877-642-7889).

Questions concerning FBI NICS E-Check that do no require an immediate response can be E-mailed to: **a_nics@leo.gov.**

Written communications can be sent to:

NICS Customer Service
Attn. FBI NICS E-Check
PO Box 4278
Clarksburg, WV 26302-4278

4 USER OBLIGATIONS

To obtain FBI NICS E-Check access, all users must agree to the following terms and conditions statement that appears on the FBI NICS E-Check Web site.

United States Department of Justice

Federal Bureau of Investigation

National Instant Criminal Background Check

E-Check Computer System

-- !! WARNING !! --

You are now accessing a nonpublic "protected computer" system, which is the property of the United States Department of Justice. Use of this computer system is reserved exclusively to the United States Government and those expressly authorized by the FBI for specific purposes permitted or required by law. **By accessing and/or using this computer system, you understand, acknowledge and agree that** ------

All data transmitted to or from this computer system, including any stored data resulting from such a transmission, is and at all times remains the property of the United States Government. All such data and transmissions are subject, at the unfettered discretion of the United States Government or any agency or authorized agent thereof, to **monitoring**, copying, interception, recording, tracking, disclosure, alteration, retrieval or destruction for any purpose (including but not limited to criminal prosecution);

You have no expectation of privacy or property interest in any data transmitted to or from this computer system;

Unauthorized or attempted unauthorized access to this computer system, or exceeding or attempting to exceed authorized access to this system is a criminal violation of the law, including Section 1030 of Title 18 of the United States Code;

Misuse or unauthorized access to this system may also result in a fine not to exceed $10,000 and/or cancellation of user privileges as set forth in 28 Code of Federal Regulations 25.11; and

As a precondition to your continued access and use of this computer system, if otherwise authorized, you will regularly review, be charged with knowledge of, and shall be deemed to have agreed to all existing and future "Monitoring/Terms and Conditions" notices posted on this computer system, as well as all responsibilities and procedures set forth in the NICS Operation Center Federal Firearms Licensee User Manual, Federal Firearms Licensee registration form and all other policies, laws and regulations regarding the NICS and/or this computer system.

4.1 User Security Responsibilities

Additionally, all users are required to accept the following term of the subscriber agreement prior to downloading their digital certificate:

By downloading this certificate you agree to accept the terms and conditions contained in the FBI NICS E-Check Subscriber Agreement listed below:

- Acknowledge that all information and representations made by you in this digital certificate are accurate.
- Accurately represent yourself in all communications with the FBI.
- Notify NICS Operations Center immediately of any change to the information contained in this digital certificate that occurs during the certificate's validity period.
- Take precautions to prevent loss, disclosure, or unauthorized use of this digital certificate and the associated private key.
- Notify NICS Operations Center to revoke this digital certificate promptly upon any actual or suspected loss, disclosure, or other compromise of this digital certificate and the associated private key immediately or within four hours upon suspicion that the private key associated with this digital certificate has been compromised or lost.
- Ensure that no unauthorized person has access to this digital certificate and the associated private key.
- Notify NICS Operations Center when this digital certificate is no longer in use or if this digital certificate becomes inoperable.
- Use this digital certificate exclusively for authorized and legal purposes associated with NICS and FBI NICS E-Check policies.

A user who is found to have acted in a manner counter to these obligations may have their digital certificate revoked without notice, thus terminating all system access privileges.

If you do not wish to agree to the terms of the Subscriber Agreement listed above, you should *not* download your FBI NICS E-Check digital certificate.

NOTE: You can only download a digital certificate from the browser and computer that you used to make the digital certificate request. If you get the error message "The Private Key for this certificate cannot be found in your key database," you will not be able to download the digital certificate from your current browser/machine combination. Possible reasons why you would get this message include;

- Using a different computer than the one from which you made the request.
- Logging on to your browser using a different profile name than the one used when the request was made.
- Using a different browser than the one used to make the request (for example, trying to download the digital certificate using Internet Explorer and when the request was made using Netscape).
- The computer operating system or browser software may have been re-installed.

Other user responsibilities may include:

- Protect passwords
- Protect unattended Personal Computers
- Utilize E-Check for authorized use only

If a certificate is no longer in use (such as when an employee leaves the FFL business) or if the certificate will not be in use for a period of 90 days or longer, it is the responsibility of the FFL to contact

NICS Customer Service so that user's certificate can be handled appropriately. Certificates found not to be in use for a period of 90 days or greater will be suspended by NICS Customer Service. Certificates that have not been used for a period of 180 days or greater will be revoked. In either case, the user must contact NICS Customer Service to re-gain access privilege to FBI NICS E-Check.

If a certificate has been issued to you and you have chosen not to download it or do not accept the Terms and Conditions, please notify NICS Customer Service so that your certificate can be terminated.

4.1.1 Guidelines for Password Selection

The following are some general guidelines for the selection of user password.

1. At least 8 character in a combination of letters, numbers or special characters.
2. Choose a word not in the dictionary.
3. Do not choose a word related to you such as spouse's name, type of car or pets name.
4. Do not use spaces or breaks between characters.
5. Passwords are case-sensitive.
6. Do not use the @ or # symbols.

4.1.2 Guidelines for Password Protection

The following are some general guidelines for the protection of user passwords.

1. Do not write down or store in a computer file a password.
2. Passwords should never be shared with another user.
3. If a user forgets his or her password, notify NICS Customer Service.
4. Do not store a password as a default password in the Internet Server connection screen.

5 REQUIREMENTS FOR USERS

To use the FBI NICS E-Check system, each FFL site must have hardware (such as a personal computer), Web browser software (that will allow employees of the FFL to use the World Wide Web (WWW)), and an Internet connection. Additional details for each of these requirements are contained in the following subsections of this document.

5.1 Computer

The computer and its operating system used to access FBI NICS E-Check must be capable of running one of the FBI NICS E-Check supported Web browsers listed in Section 5.2. Additionally, the computer must be capable of connecting to the Internet through an Internet Service Provider (ISP).

Multiple FBI NICS E-Check users can share a single computer as long as the private key associated with each user's digital certificate is password protected. Procedures for protecting a digital certificate are contained in Section 6.

Web TV appliances are not supported by the FBI NICS E-Check system.

5.1.1 Computer System Time

The session cookies used by FBI NICS E-Check require reasonably accurate computer system time, date and time-zone, to be set on any computer accessing FBI NICS E-Check.

To set the system time parameters on Windows based computers:

1. Double click the **time** that is displayed on the task manager (usually located in the lower right hand corner of your screen). The "Date/Time Properties" window will appear.
2. Select the **Time Zone** tab.
3. Choose your time zone from the drop-down list.
4. Ensure that Automatically adjust clock for daylight savings changes is checked.
5. Select the **Date&Time** tab.
6. Set the year by clicking on the up or down arrows next to the year.
7. Set the month using the drop-down lists.
8. Set the day of the month by clicking on it in the calendar window.
9. Select the time field (hh:mm:ss) to be changed by clicking on it once then use the up or down arrows to increase or decrease time.
10. Once all necessary time changes have been made, click the **OK** button.

5.2 Web Browser

FBI NICS E-Check supports three of the most commonly used browsers: Netscape, Internet Explorer, and American Online. The browser must support digital certificates and provide 128-bit encryption capability. This version is commonly called the "Domestic" or "U.S" version of the browser (the International version shipped with some computers does not permit 128-bit encryption). Supported browsers and the procedure for testing version and encryption capability are listed below. Specific procedures necessary for FBI NICS E-Check usage are outlined in Section 6 for Netscape, Internet Explorer and

AOL.

5.2.1 Netscape Communicator versions 4.5x and higher

The version and encryption capability of your Netscape browsers can easily be checked for proper version and 128-bit encryption capability. If a user does not have Netscape, the browser may be obtained free of charge from the Netscape web site http://www.netscape.com

To check Netscape version and encryption capability:

1. Startup Netscape Communicator
2. From the menu at the top of the browser select **Help**, **About Communicator**.
3. A Web page appears showing the Version number at the top.
4. If the browser has 128-bit encryption, the following text will appear in bold in the left hand column of the page:

The version supports U.S. security with RSA Public Key Cryptography, MD2, MD5, RC2-CBC, RC4, DES-CBC, DES-EDE3-CBC.

5.2.2 Microsoft Internet Explorer versions 5.0 and higher

The version and encryption capability of the Internet Explorer browser can easily be checked for proper version and 128-bit encryption capability. The latest Internet Explorer browser may be obtained free of charge from the Microsoft web site http://www.microsoft.com .

To check Internet Explorer version and encryption capability:

1. Startup Internet Explorer.
2. From the menu at the top of the browser select Help, About Internet Explorer.
3. A help window appears showing the Version number and Cipher Strength.
4. Ensure that the version is listed as a FBI NICS E-Check compatible version and that the Cipher Strength is 128-bit.

Internet Explorer 5.5 includes 128-bit encryption. However, if you are running Windows 2000, you will need to also install the Windows 2000 High Encryption Pack to achieve the 128-bit cipher strength. The High Encryption Pack is available for download from the Microsoft web site, free of charge.

5.2.3 America Online (AOL) versions 5.0 and higher

AOL currently uses the Internet Explorer browser. The AOL packaged browser can be obtained from the AOL web site http://www.aol.com. Perform the steps outlined in Section 5.2.2 to check compatibility.

5.3 Internet Connection

An Internet connection to the World Wide Web is required to access the FBI NICS E-Check system. There are no special requirements for this connection. Any ISP may be used to connect to the Internet.

6 USER PROCEDURES

This section provides the specific procedures necessary for a user to login to the FBI NICS E-Check system. This section also provides information on how to protect the login access privileges from unauthorized users.

Prior to logging in to FBI NICS E-Check, the user requirements listed in Section 5 must be met. Next you must complete the multi-step process outlined in this section. The user should determine which browser they will be using and follow the steps for that specific browser. Since different browsers require different actions, this section has been separated into three Sections:

Section 6.1

This section contains the FBI NICS E-Check enrollment process and must be completed by all users wishing to access the FBI NICS E-Check system.

Section 6.2

This section is for users choosing to use the **Netscape** browser only. These procedures have been written for Netscape version 4.78. Other Netscape versions may require slightly different actions.

Section 6.3

This section is for users choosing to use the **Internet Explorer** browser only. These procedures have been written for Internet Explorer version 5.5 (Service Pack2). Other Internet Explorer versions may require slightly different actions.

AOL users will access the Internet via their AOL account. Once the connection has been established, the AOL user will minimize the AOL screen and follow the Internet Explorer procedures in Section 6.3.

6.1 FBI NICS E-CHECK Enrollment Step 1

Every FFL will receive an enrollment package from the NICS Section, which will include a NICS/E-Check enrollment form. This form must be filled out, signed, and the original copy returned to:

NICS Customer Service
Attn. NICS E-Check
PO Box 4278
Clarksburg, WV 26302-4278

1. A form must be completed, for every individual requiring access to FBI NICS E-Check.
2. Every returned form must contain both the signature of the applying user and the witnessing FFL.
3. You may copy the form to use for additional applicants or download it from https://forms.nicsezcheckfbi.gov (be sure to include the "s" in https).

NOTE: NICS Customer Service must receive the original signed copy. Faxing or E-mailing of the enrollment form will not be accepted. Access to FBI NICS E-Check will not be granted unless NICS Customer Service receives the original signed copy of the enrollment form.

6.2 Netscape Procedures

6.2.1 Netscape Communicator Profiles Procedures—Step 2

NOTE: If you have previously setup profiles in Netscape, go to Step 11 below.

1. Startup the User Profile Manager by launching **Start**, **Programs**, **Netscape Communicator**, **Utilities**, **User Profile Manager**. The Profiles manager window will appear.
2. Click the **New…** button to create a new profile.

NOTE: Netscape cannot be running when attempting to start the User Profile Manager. If you get an error message stating "Please exit out of Netscape Communicator in order to run the Profile Manager" click the **OK** button on that window, close Netscape and return to Step 1.

3. The "Creating a New Profile" window appears. Click the **Next** button.
4. Enter your name in the "Full Name:" box and your E-mail address (if available) in the "Email Address" box. If E-mail is not available, leave it blank.
5. Click the **Next** button.
6. Choose a profile name to identify your profile and enter it in the "Profile Name:" box; for example, your name. Do not modify the default directory in the lower box (i.e. C:\Program Files\Netscape\User*your_profile_name*). Click the **Next** button.
7. The "Set up your Outgoing Mail Server" window will be displayed. You may finish the setup by clicking the **Finish** button since Netscape Communicator now has enough information to setup your basic profile.
8. Or, after clicking the **Finish** button in the previous step, Netscape will startup using your new profile. From this point on, you will be prompted to select a Profile Name when starting Netscape.
9. If you know your E-mail information and wish to configure E-mail, you may continue to enter it by clicking the **Next** button instead of the **Finish** button.

NOTE: If Netscape starts and you are not connected to the Internet, you may see a message stating that "Netscape is unable to locate the server ….Please check the server name and try again." If this occurs, click the **OK** button in the message window.

10. Proceed to Enabling Session Cookies.
11. If Communicator has been previously configured to use personal profiles, you will see the "Profile Manager" window similar to the one below when starting Netscape.

If this window appears and you do not already have a Profile Nameset up, click the **Manage Profiles** button and go to step 2 above to configure your profile. If you already have a Profile Name, skip to Enabling Session Cookies below.

6.2.1.1 Enabling Session Cookies

A cookie is a piece of information that is sent to your browser when you access certain sections of the FBI NICS E-Check Web site. The purpose of a cookie is to store information that is submitted to the FBI NICS E-Check system. FBI NICS E-Check uses a particular type of cookie called a session cookie that is only used during the current session and not for subsequent sessions. The cookies used by FBI NICS E-Check, timeout after 15 minutes of user inactivity, which require the user to re-login. A cookie alone cannot read information from your computer. The only information stored in the cookie is information submitted to the FBI NICS E-Check Web site. Also, information stored in cookies placed by FBI NICS E-Check cannot be seen by other Web sites on the Internet. **Session cookies must be enabled in your browser to login to the FBI NICS E-Check system.**

To enable session cookies:

1. If Netscape is not already running under your profile, start it and choose your personal profile name from the "Profile Manager" drop down list, then click the **Start Communicator** button.
   a) If there is only one Netscape personal profile configured on the computer, the "Profile Manager" window will not be displayed when starting Netscape.
   b) It is not necessary to connect to the Internet to enable session cookies.
   c) System time needs to be correctly set on your computer for cookies to work properly. See Computer System Time (section 5.1.1).
2. Choose **Edit, Preferences…** from the menu at the top of the Netscape browser window.
   Note: If you have Netscape version 6.0 or higher, in the Preferences window, under Privacy and Security click Cookies. Choose Enable all Cookies then OK. Skip to Step 15.
3. Select the **Advanced** category.
4. Ensure that "**Accept all cookies**" is selected.
5. Click the **OK** button in the "**Preferences**" window. Close Netscape.
6. Proceed to Section 6.2.2. Requesting a Digital Certificate—Step 3.

6.2.2 Requesting a Digital Certificate—Step 3

NOTE: Do not proceed to this step, until your enrollment form has been sent to NICS as described in Section 6.1 FBI NICS E-Check Enrollment—Step 1. Your digital certificate request cannot be processed until NICS has received and processed the enrollment form. Only one digital certificate will be issued to an individual. Subsequent digital certificate requests will be ignored.

1. Connect to the Internet through an Internet Service Provider (ISP) using the same computer that will be used later to login to the FBI NICS E-Check system.
2. If Netscape is not already running under your profile, start it and choose your personal profile name from the "Profile Manager" drop down list, then click the **Start Communicator** button.
   NOTE: if there is only one Netscape personal profile is configured on your computer, the "Profile Manager" window will not be displayed when starting Netscape.
3. Go to the Web address https://register.nicsezcheckfbi.gov (be sure to include the "s" in

https).

4. The first of five "New Site Certificate" windows will be displayed indicating that you are connecting to a secure site that Netscape has not connected to before. Click the **Next** button on the first three widows.
5. On the fourth window, "uncheck" the box **Warn me before I send information to this site** and click the **Next** button.
6. On the fifth window, click the **Finish** button.
7. A "Security Information" window may appear stating that you have requested a secure document. If this occurs, click the **Continue** button.
8. The "Terms and Conditions" window appears. Read this carefully. To accept the terms and conditions, click the **AGREE** button, or click the **DISAGREE** button and exit FBI NICS E-Check.
9. Choosing agree, will display the "FBI NICS E-Check Online Enrollment Server" Web page. This page has three links. Click the link **Download the FBI NICS E-Check Certificate Authority digital certificate**. This is done so that the browser recognizes and trusts the FBI NICS E-Check Web site. Choose **Open** and **OK**.
10. The first of six "New Certificate Authority" windows will be displayed. Click **Next** on the first three windows.
11. On the fourth "New Certificate Authority" window, click the **"check"** box **"Accept this Certificate Authority for certifying network sites"** and click the **Next** button.
12. On the fifth "New Certificate Authority" window, click the **Next** button.
13. On the sixth and final "**New Certificate Authority**" window, type **NICS E-Check** in the "Name: box and click the **Finish** button.
14. Click the link **Request an FFL digital certificate.** You are presented with the "FBI NICS E-Check Online Certificate Request form" Web page.
15. Enter information on the online registration form, being sure to fill in all required fields as denoted by the red asterisks.
    NOTE: The fields on the online form are case sensitive (you may use upper or lower case letters). Make certain that your FFL number, codeword, name, E-mail address, and business phone number are correct. If you do not have an e-mail address, leave it blank.
16. Once all the information is entered, click the Submit button.
17. The information submitted is automatically checked for completeness and correctness. If the information entered is correct, the "Please Verify Your Information" page should appear. Proceed to step 18.
    If there was a problem with the submitted information, a page stating "ERROR: Bad or not enough information" will appear. A message may also be displayed on this page stating what information has a problem. You may correct the information on this page and click the **Proceed** button. Your information will be checked again.
    *NOTE: One such error that could occur is that another FBI NICS E-Check user has already chosen the same username. If this error happens, enter a different username and click the **Proceed** button.*
18. Review the information presented on the "Please Verify Your Information" page. If the information is satisfactory, proceed to the next step. If corrections are necessary, click the **Make Corrections** button. Make the necessary corrections and click the **Proceed** button. Continue this process until you are satisfied with the information presented, then continue.
19. Make sure that the "Key Size" at the bottom of the page is "1024 (High Grade)". If not, change this value using the drop down selection. Click the **Submit** button.
20. A window will appear stating that a private key will be generated. Click the **OK** button. The

"Setting Up Your Communicator Password" window will appear prompting you to enter a password in the "Password:" box to protect your Communicator Certificate Database (DB) (This assumes that your profile has not previously been password protected. If it has, enter your existing password). In the "Type it again to confirm" box, re-enter your password and click the **OK** button. (See Section 4.1.1) The page stating that "Your request has been forwarded to E-Check" will be displayed, completing the digital certificate request process. *NOTE: **Remember your password!** NICS Customer Service has no knowledge of user passwords. However, if your password is forgotten, contact NICS Customer Service for further instructions.*

21. You may now close the browser.

Your online digital certificate application has now been submitted to the NICS Customer Service for evaluation. NICS Customer Service requires the signed original FBI NICS E-Check Enrollment form as well as the online digital certificate request. Allow time for NICS Customer Service to process any digital certificate request. This period is usually 3 to 5 business days after NICS Customer Service receives your FBI NICS E-Check Enrollment form. During this time period, information submitted online, the original signed enrollment form, and other FFL information on file at NICS will be reviewed to determine whether a digital certificate will be issued in response to the digital certificate request. NICS will attempt to notify you by E-mail or telephone once your request has been processed.

You must wait for notification that your digital certificate has been issued before proceeding to "Downloading Your Digital Certificate". If the user specified an E-mail address in the request, they will be notified via E-mail. If an E-mail address was not specified, NICS Customer Service will notify the user via telephone.

If the user has not been notified that the certificate request has been processed after 10 days following the mailing of the enrollment form and submitting the online certificate request, contact NICS Customer Service.

6.2.3 Downloading Your Digital Certificate—Step 4

STOP! Do not perform this step until you have been notified by NICS that your digital certificate is available to download.

A digital certificate, once issued, must be downloaded from FBI NICS E-Check and installed in the same browser and profile that was used to generate the digital certificate request. For example, a user cannot generate a digital certificate request with Netscape and download the issued digital certificate into Internet Explorer. Also, you cannot generate a digital certificate request from your business computer and download the issued digital certificate using your home computer. There are other ways to move digital certificates between computers and browsers discussed in the Exporting and Importing sections of this user's guide.

E-mail is the preferred method of notifying a user that a digital certificate request has been processed. Telephone notification will be used for those requests that did not contain an E-mail address. Both options are outlined below. Users should follow the steps pertaining to the option used for their request.

6.2.3.1 E-mail Notification Method

The E-mail address entered in the request must be accessible from the computer where the digital cer-

tificate request was generated. The E-mail notification will contain a link and instructions to download your digital certificate.

To download your digital certificate:

1. Connect to the Internet through your Internet Service Provider (ISP) using the same computer, which was used to generate your digital certificate request.
2. Check your E-mail for a message from register@nicsezcheckfbi.gov.
3. Read the subscriber agreement contained in E-mail before downloading.
4. If you accept the terms of the subscriber agreement, click on the link contained in the E-mail. The "Password Entry Dialog" box may appear.
5. If this happens, enter your Communicator Certificate DB password. This will be the same password that was entered in Request Your Digital Certificate section above. Passwords are case sensitive. Click the **OK** button.

6.2.3.2 Telephone Notification Method

If an E-mail address was not entered with your online digital certificate request, NICS Customer Service will contact you by telephone when your digital certificate request has been processed. To download your certificate after notification by telephone:

1. Connect to the Internet through an ISP using the same computer that was used to generate the digital certificate request.
2. If Netscape is not already running, double-click the **Netscape** icon, choose your personal profile from the "Profile Manager" drop-down list and click **Start Communicator**.
   NOTE: if there is only one personal profile configured, Netscape does not display the "Profile Manager" window when starting.
3. Go to the Web address https://register.nicsezcheckfbi.gov (be sure to include the "s" in https). A "Security Information" window may appear stating that you have requested a secure document. If this occurs, click the **Continue** button.
4. The "Terms and Conditions" page appears. Read this carefully. To accept the terms and conditions, click the **AGREE** button, or click the **DISAGREE** button to exit.
5. The "FBI NICS E-Check Online Enrollment Server" Web page appears. This page has three links. Click on the link **Download Your FFL digital certificate.**
6. The "FBI NICS E-Check FFL Digital Certificate Search" page appears.
7. Enter your First and Last Name (as you entered it on the request), and your FFL number. Click the **Submit** button.
8. A page should be displayed stating, "At least one digital certificate was found that matched your input". Read the subscriber agreement found on this page.
9. If you choose to accept the subscriber agreement proceed to download your digital certificate by scrolling to the list of digital certificates found on the bottom of the page. Usually this list will have only a single entry, but multiple digital certificates could be displayed. If no digital certificates matching the search criteria were found, you will be prompted to try another search.
   NOTE: If there are other FBI NICS E-Check users at an FFL location that have the same name, the name that appears in the digital certificate will be appended with a number. For example, if there are two John Smith's, one will be identified as John Smith-1 (the first John Smith will be identified as John Smith). NICS Customer Service will alert the user to this when providing notification that the digital certificate has been issued.

10. Click on the **Download Certificate** link next to your name.
11. A window will appear stating that Netscape is attempting to download the digital certificate. Click the **OK**.
    The "Password Entry Dialog" box may appear. If this happens, enter your Communicator Certificate DB password. Click **OK**. This will be the same password that was entered in step 20 of the Request a Digital Certificate section above.

NOTE: If you attempt to download a digital certificate that is not yours, you will get an error. If this happens, select a different link in the digital certificate list of step 9 above or call NICS Customer Support.

6.2.3.3 Verification

Regardless of the method of notification, the user should ensure that the digital certificate has been installed and set up for use.

To verify certificate installation:

1. Select the **Security** icon (it looks like a lock) from the Netscape menu bar at the top of the Netscape window.
2. The "Security Info" page will appear. Select **Yours** under certificates.
3. Ensure that there is an FBI ID digital certificate in the list "This is your certificate:" indicating the successful download of your FBI NICS E-Check digital certificate.
4. In the same window, click on **Navigator**.
5. In the drop-down "Certificate to identify you to a Web site:" choose **Select Automatically.** This allows Netscape to associate the correct digital certificate with the correct web site if the user has other digital certificates that are being used for other purposes.
   NOTE: If for some reason, a user has multiple FBI NICS E-Check digital certificates under the same profile, the user must choose the digital certificate that they wish to present to the FBI NICS E-Check Web site in step 5 above instead of choosing ***Select Automatically****.*
6. Click the **OK** button. After downloading and verifying the digital certificate, proceed to Section 6.2.4. Session Log on—Step 5.

6.2.4 Session Log on—Step 5

1. Connect to the Internet through your Internet Service Provider (if not already connected).
2. If Netscape is not already running **under your profile**, start it and choose your profile from the "Profile Manager" drop down list and click **Start Communicator.**
   NOTE: If there is only one personal profile configured, Netscape does not display the "Profile Manager" window when starting. If Netscape is already running, you must ensure that it is running under your profile, as you cannot use another individuals digital certificate to access FBI NICS E-Check. You can ensure that it is running under your profile by selecting ***Bookmarks, Edit Bookmarks….*** *The Bookmarks window will open displaying the directory tree of your bookmarks. The top of the tree will display* ***"Bookmarks for your profile name"****. Ensure your profile name is the one you created in Step 2—Setting Up Netscape Communicator Profiles. Close the Bookmarks window and proceed.*
3. Go to https://www.nicsezcheckfbi.gov (be sure to put the "s" in https). A "Security Information" window may appear stating that you have requested a secure document. If this occurs, click the **Continue** button.

4. The "Password Entry Dialog" box may appear. If this happens, enter your Communicator Certificate DB password. This will be the same password that was entered in step 20 of the Request Your Digital Certificate section above. Passwords are case sensitive. Click the **OK** button.
5. The FBI NICS E-Check "Notice" page will be displayed. Click **Continue.**
6. At this point, the **Terms and Conditions** page appears. Read this carefully. Click the **AGREE** button to continue, or click the **DISAGREE** button to exit FBI NICS E-Check.
7. The FBI NICS E-Check Login page will be displayed. Enter the proper FFL number, code-word, username and phone number (including area code) and click the **Submit** button.
8. If login was successful, the FBI NICS E-Check search request page will be displayed.
9. If login was unsuccessful, the user will be returned to the login page where a retry can be done.

6.2.5 Session Logoff

1. While logged in, click **EXIT** on top of any FBI NICS E-Check page.
2. The Terms & Conditions page will appear.
3. Close the Netscape browser to ensure that no other individual may access your digital certificate.

6.2.6 Exporting Your Digital Certificate

The digital certificate that was downloaded from FBI NICS E-Check can only be used on the browser and profile that was used to download the digital certificate unless special procedures are followed. Once downloaded, the digital certificate can be copied to other computers or browsers for use. The process of copying a digital certificate from its usual location (inside a browser's database) to another location (i.e. floppy diskette, windows folder, etc.) is called exporting. The digital certificate may still be used from its original location once it has been exported because the process of exporting only generates a copy of the original digital certificate.

It is also a good idea to backup important digital certificates and its "private key" to a floppy diskette so that it may be recovered in the event of a computer failure. Backing up a digital certificate is accomplished through the exporting process.

To export and backup a digital certificate:

1. Startup Netscape using your profile.
2. Click on the lock icon (located at the top of the browser) to open the "Security Info" page.
3. Under Certificates, click on **Yours**.
4. A list of the user's digital certificates will appear in the box to the right. Highlight the appropriate FBI digital certificate by clicking on it once, then click **Export**.
5. The "Password Entry Dialog" windows will appear. Enter your Communicator Certificate DB password (created in step 20 - Requesting Your Digital Certificate) and click the **OK** button.
6. The second "Password Entry Dialog" window appears. Enter a password that will be used to protect the exported digital certificate (you can use your Communicator Certificate DB password) and click the **OK** button.
7. A third "Password Entry Dialog" window appears. Re-enter the password entered in step 6

above and click the **OK** button.
NOTE: **Remember your password!** NICS Customer Service has no knowledge of user passwords. However, if your password is forgotten, contact NICS Customer Service for further instructions.

8. You will be prompted for the file name and the destination for the exported digital certificate. Insert a floppy diskette into your computer. In the "Save in:" box click the down arrow to **select 3 ½ Floppy (A:)** (You could also export to other locations such as your hard-drive, CD, Zip drive, etc.)
9. In the "File name:" box type a name to identify the digital certificate. Click the **Save** button.
10. The digital certificate file will be exported to the designated drive, and a small window will be displayed stating "Your certificate has been successfully exported". Click on the **OK** button.

The digital certificate has now been exported. Remove the floppy diskette from the computer and proceed to import the digital certificate to another computer or store it for a digital certificate backup.

6.2.7 Importing a Digital Certificate

The process of copying a digital certificate into a browser from a file is called importing. A user may need to import a digital certificate that was previously exported in the event of a computer crash or if moving the certificate to another computer.

To import a digital certificate:

1. Start Netscape using your profile.
2. Click on the lock icon (located at the top of the browser) to open the "Security Info" page.
3. Under Certificates, click on **Yours**.
4. Insert the media containing the exported digital certificate i.e., Cd, tape, diskette.
5. Click **Import a Certificate**…
6. The "File Name to Import" window appears. Click the drop down box **Look in:** and select the **3½" Floppy (A:)** (or other source from which you may be importing).
7. The digital certificate exported earlier appears in the box. Select the digital certificate by clicking on it once. Click **Open**.
8. The "Password Entry Dialog" window appears requesting the password protecting the imported data. Enter the password set in Exporting step 5 and click the **OK** button.
9. A small window will appear stating, "Your certificate has been successfully imported." Click the **OK** button.
10. Click the **OK** button on the "**Your Certificates**" window that remains on the browser.

6.2.8 Viewing a Digital Certificate

Once downloaded, the user may view the digital certificate and its content at any time.

To view a digital certificate:

1. Click the **Security** icon (the lock) from the Netscape menu bar.
2. The "Security Info" page will appear. Select **Yours** under certificates.
3. Highlight the appropriate FBI NICS E-Check digital certificate by clicking on it once.
4. Click the **View** button. A window will be displayed showing the digital certificate's content.

5. Click **OK**.

6.2.9 Removing a Digital Certificate

It may become necessary to remove a FBI NICS E-Check digital certificate. The following procedure can be used to permanently remove a FBI NICS E-Check digital certificate.

To remove a digital certificate:

1. Start Netscape using your profile.
2. Click the Security icon (the lock) from the Netscape menu bar.
3. The "Security Info" page will appear. Select **Yours** under certificates.
4. Select the digital certificate that you wish to delete and click the **Delete** button.
5. The "Delete a Personal Certificate" window will appear warning, "if you delete this Certificate you will not be able to read any E-mail that has been encrypted with it". Click the **OK** button in this window.
6. Click the **OK** button on the "Your Certificates" window that remains on your desktop.

6.2.10 Removing A Netscape Profile

Removing a user Netscape Profile removes all browser settings, digital certificates and their associated private keys stored by that user. This process is useful for removing FBI NICS E-Check system access when a user has left a particular organization. The following procedure can be used to permanently remove a user's Netscape profile.

NOTE: Netscape cannot be running when attempting to start the User Profile Manager. If you get an error message stating "Please exit out of Netscape Communicator in order to run the Profile Manager" click the OK button on that window, close Netscape and begin at step1 below.

To remove a Netscape profile:

1. Start the User Profile Manager by clicking Start, Programs, Netscape Communicator, Utilities, User Profile Manager.
2. The Profile Manager window will appear.
3. Select the profile that you wish to delete and click the **Delete** button.
4. The "Delete Profile" window will be displayed asking you if you wish to delete the profile directory and all the files in it. Click the Delete Directory button.
5. The profile has now been deleted and should no longer appear in the Profile Manager list. Close the "Delete Profile" window and Exit the "Profile Manager".

6.2.11 Digital Certificate Expiration and Rekey Request

To further enhance the security of issued digital certificates, each digital certificate has an expiration date imposed upon it making it useful for a specified period of time. This time period is known as the validity period of the digital certificate. Typically, validity periods will range from 1 year to 18 months. Once a digital certificate has expired, it can no longer be used to obtain FBI NICS E-Check access. Thirty days prior to the end of the validity period, NICS Customer Service will contact the user. Upon notification, the user must submit an online digital certificate request and obtain a new certificate through the process outlined in section 6.2.2 above. However, it is not necessary to submit another

NICS/E-Check FFL Enrollment form unless the certificate has expired or been revoked.

To view your certificate's validity period:

1. Start Netscape using your profile.
2. Click on the lock icon (located at the top of the browser) to open the "Security Info" page.
3. Under Certificates, click on **Yours**.
4. A list of the user's digital certificates will appear in the box to the right. Highlight the appropriate FBI digital certificate by clicking on it once, then click **View.**
5. Various information about your certificate will be displayed. Look for the validity time period in the bold line with the following format: **"This Certificate is Valid from Day MMM DD, YYYY to Day MMM DD, YYYY"**

6.3 Internet Explorer Procedures—Step 2

If you are using Internet Explorer version 6.0 or higher, please skip to section 6.3.1.1 Enabling Session Cookies-Step 2a.

6.3.1 Enabling Session Cookies

A cookie is a piece of information that is sent to your browser when you access certain sections of FBI NICS E-Check Web site. The purpose of a cookie is to store information that you submit to the FBI NICS E-Check system. FBI NICS E-Check uses a particular type of cookie called a session cookie that is only used during the current session and not for subsequent sessions. The cookies used by FBI NICS E-Check, timeout after 15 minutes of user inactivity, which requires the user to re-login. A cookie alone cannot read information from your computer. The only information stored in FBI NICS E-Check cookies is information you submit to the FBI NICS E-Check Web site. Also, information stored in cookies placed by FBI NICS E-Check cannot be seen by other Web sites on the Internet. **Session cookies must be enabled in your browser to login to FBI NICS E-Check.**

To enable session cookies for versions earlier than 6.0:

1. Start Internet Explorer, but it is not necessary to connect to the Internet to enable session cookies.
2. From the menu at the top of the Internet Explorer window, choose **Tools, Internet Options**.
3. The "Internet Options" window appears. Select the **Security** tab.
4. Select the "Internet" zone icon and click the **Custom Level…** button.
5. The "Security settings" window will appear. Scroll down to the **Cookies** section and select **Enable** underneath the "Allow per-session cookies (not stored)" section.
6. Click the **OK** button on the "Security settings" window.
7. A "Warning" window should appear asking, "Are you sure you want to change the security settings for this zone?" Click the **Yes** button in this window.
8. Click the **OK** button in the "Internet settings" window.
9. Proceed to Section 6.3.2. Requesting a Digital Certificate Using I.E.—Step 3.

6.3.1.1 Internet Explorer Procedures 6.0 or Higher: Enabling Session Cookies—Step 2a

1. Start Internet Explorer, but it is not necessary to connect to the Internet to enable session

cookies.
2. From the menu at the top of the Internet Explorer window, choose Tools, Internet Options.
3. Click the Privacy tab and then click Advanced.
4. Ensure the Override Auto Cookie Handling check box is checked.
5. Ensure Accept is selected under First-Party Cookies and Third-Party Cookies.
6. Ensure that Always Allow Session Cookies is checked.
7. Click OK and close the browser.

6.3.2 Requesting a Digital Certificate Using I.E.—Step 3

NOTE: Do not proceed to this step, until your enrollment form has been sent to NICS as described in Step 1. Your digital certificate request cannot be processed until NICS has received and processed the enrollment form. Only one digital certificate will be issued to an individual. Subsequent digital certificate requests will be ignored.

1. Connect to the Internet through an Internet Service Provider using the same computer that will be used to login to the FBI NICS E-Check system.
2. Start Internet Explorer if it is not already running.
3. Go to the Web address https://register.nicsezcheckfbi.gov (be sure to include the "s" in https).
4. Depending on the browser's settings, a security alert may be displayed indicating that a connection to a secure site is being made. If this occurs, click the **OK** button.
5. Another security alert window will be displayed stating "the security certificate was issued by a company you have not chosen to trust." It then asks, "Do you want to proceed?" Click the **YES** button indicating that you have chosen to temporarily trust the FBI NICS E-Check web site.
6. At this point, you are presented with the "Terms and Conditions" page. Read this carefully. To accept the terms and conditions, click the **AGREE** button, or click the **DISAGREE** button and exit FBI NICS E-Check.
7. The "FBI NICS E-Check Online Enrollment Server" Web page is displayed. This page has three links. Click the link **Download the FBI Certificate Authority certificate**. This process will allow the browser to permanently trust the FBI NICS E-Check web site.
   NOTE: If another user has already performed Downloaded the FBI Certificate Authority certificate into the Internet Explorer browser, it is not necessary to repeat step 7.
8. The "File Download" window appears stating, "you have chosen to download a file from this location". It asks, "what would you like to do with this file?" Choose; **Open this file from its current location** and click the **OK** button.
9. The "Certificate" window will be displayed. Click the **Install Certificate** button.
10. A "Certificate Import Wizard" window will appear. Click the **Next** button.
11. Another "Certificate Import Wizard" window will be displayed. Ensure that Automatically select a certificate store… is selected and click the Next button.
12. The final "Certificate Import Wizard" window appears stating "Completing the Certificate Import…." Click the **Finish** button on this window.
13. A small window will be displayed stating that the Import was successful. Click the **OK** button in this window.
14. Click **OK** on the "Certificate" window that remains on your desktop to close the window.
15. Next click the link Request an FFL digital certificate on the "FBI NICS E-Check Online Enrollment Server" Web page.

16. The "FBI NICS E-Check Online Digital Certificate Request Form" is displayed. Enter information in the online registration form, being sure to fill in all required fields as denoted by the red asterisks. Disregard the profile portion of the online form.
    NOTE: The fields on the online form are case sensitive (you may use upper or lower case letters). Make certain that your FFL number; codeword, name, E-mail address, and business phone number are correct. If you do not have an e-mail address, leave it blank. The Username field requires a 6 to 10 character (letters, numbers or both) username. Choose a username that you will remember as this will be used by you when logging into FBI NICS E-Check. Do not share your username with anyone!
17. Once all the information is entered, click the **Submit** button at the bottom of the page.
18. The information submitted is automatically checked for completeness and correctness. If the information was entered correctly, the message "Your request has been forwarded to E-Check" is displayed at the top of the screen. This completes the digital certificate request process.
19. If there was a problem with the information that was submitted, a page stating "Incorrect or Missing Information" will be returned. A bulleted message may also be displayed on this page stating the error. After reading the bulleted message, click the **Back** button on the browser toolbar to return to the previous page to make any changes.
    NOTE: One such error that could occur is that another FBI NICS E-Check user has already chosen the username you chose. If this happens, you will need to choose a different username and try again.
20. Make all the necessary corrections and click the **Submit** button. Continue this process until the page stating that "Your request has been forwarded to FBI NICS E-Check" is displayed. This completes the digital certificate request process.
21. Close the browser.

6.3.2.1 Requesting a Certificate Using Internet Explorer 6.0 or Higher—Step 3a

1. Connect to the Internet through an Internet Service Provider using the same computer that will be used to login to the FBI NICS E-Check system.
2. Start Internet Explorer if it is not already running.
3. Go to the Web address https://register.nicsezcheckfbi.gov (be sure to include the "s" in https).
4. Depending on the browser's settings, a security alert may be displayed indicating that a connection to a secure site is being made. If this occurs, click the **OK** button.
5. Another security alert window will be displayed stating "the security certificate was issued by a company you have not chosen to trust." It then asks, "Do you want to proceed?" Click the **YES** button indicating that you have chosen to temporarily trust the FBI NICS E-Check web site.
6. At this point, you are presented with the "Terms and Conditions" page. Read this carefully. To accept the terms and conditions, click the **AGREE** button, or click the **DISAGREE** button and exit FBI NICS E-Check.
7. The "FBI NICS E-Check Online Enrollment Server" Web page is displayed. This page has three links. Click the link **Download the FBI Certificate Authority certificate**. This process will allow the browser to permanently trust the FBI NICS E-Check web site.
   NOTE: If another user has already performed Downloaded the FBI Certificate Authority certificate into the Internet Explorer browser, it is not necessary to repeat step 7.
8. Click **Save As**.

9. Click the **.xuda** file.
10. Click **Save**. Window will appear stating that the download is complete.
11. Click **Close**.
12. Then, click **Tools, Internet Options, Content Tab, Certificates**. The Certificate Manager window appears and click Import. The Certificate Manager Import Wizard window appears.
13. Click **Next**. Click the **Browse** button.
14. From the File Types drop-down list box, choose **All Files**.
15. Find the **.xuda** file that you named in step 9 and click **open**.
16. Click **Next** and **Next** again.
17. Click **OK** then click **Close**. Click **OK**.

The online digital certificate application has now been submitted to the NICS Customer Service for evaluation. NICS Customer Service requires the signed original FBI NICS E-Check Enrollment form as well as the online digital certificate request. Allow time for NICS Customer Service to process the digital certificate request. This period is usually 3 to 5 business days after NICS Customer Service receives the FBI NICS E-Check Enrollment form. During this time period, information submitted online, the original signed enrollment form, and other FFL information on file at NICS will be reviewed to determine whether a digital certificate will be issued in response to the digital certificate request. NICS will attempt to notify the user by E-mail or telephone once the request has been processed.

The user must wait for notification that the digital certificate has been issued before proceeding to Section 6.3.3. Downloading Your Digital Certificate—Step 4. If an E-mail address was specified in the request, notification will be via E-mail. If an E-mail address was not specified, NICS Customer Service will notify the user via telephone.

If the user has not been notified that the certificate request has been processed after 10 days following the mailing of the enrollment form and submitting the online certificate request, contact NICS Customer Service.

6.3.3 Downloading Your Digital Certificate—Step 4

STOP! Do not perform this step until you have been notified by NICS that your digital certificate is available to download.

A digital certificate, once issued, must be downloaded from FBI NICS E-Check and installed in the same browser that was used to generate the digital certificate request. For example, a digital certificate request cannot be generated with Netscape and downloaded using Internet Explorer. Also, a digital certificate request cannot be generated from your business computer and download using your home computer. There are other ways to move digital certificates between computers and browsers discussed in the Exporting and Importing sections of this user's guide.

E-mail is the preferred method of notifying a user that a digital certificate request has been processed. Telephone notification will be used for those requests that did not submit an E-mail address. Both options are outlined below.

6.3.3.1 E-mail Notification Method

The E-mail address that was entered on the request must be accessible from the computer where the digital certificate request was generated. The E-mail notification the user receives will contain a link and

instructions to download his or her digital certificate.

To download a digital certificate from e-mail notification:

1. Connect to the Internet through an Internet Service Provider using the same computer used to make the user digital certificate request.
2. Check your E-mail for a message from register@nicsezcheckfbi.gov.
3. Read the subscriber agreement contained in the E-mail before downloading.
4. To accept the terms of the subscriber agreement, click on the link contained in the E-mail.
5. The "Certificate Download" page will be displayed showing the contents of the digital certificate. Scroll to the bottom of this page and click the **Install Client Certificate** button.
6. Click the **Install** button on the next page that is displayed.
7. A small window will be displayed stating "Your new certificate has been successfully installed!". Click the **OK** button.
8. Proceed to Section 6.3.4. Protecting Your Digital Certificate and Private Key—Step 5.

6.3.3.2 Telephone Notification Method

If an E-mail address was not entered with the online digital certificate request, NICS Customer Service will contact the user by telephone when the digital certificate request has been processed.

To download a digital certificate from telephone notification:

1. Connect to the Internet through an Internet Service Provider using the same computer used to generate your digital certificate request.
2. Start Internet Explorer if it is not already running.
3. Go to the Web address https://register.nicsezcheckfbi.gov (be sure to include the "s" in https).
4. Depending on the browser's settings, a security alert may be displayed indicating that connection to a secure site is being made. If this occurs, click the **OK** button.
5. The "Terms and Conditions" page appears. Read this carefully. To accept the terms and conditions, click the **AGREE** button, or click the **DISAGREE** button to exit.
6. The "FBI NICS E-Check Online Enrollment Server" Web page is then presented. This page has three links. Click on the link **Download Your FFL digital certificate.**
7. The "FBI NICS E-Check FFL Digital Certificate Search" page is displayed.
8. Enter the user First and Last Name (as entered in the digital certificate request), and the FFL number. Click the **Submit** button.
9. A page will be displayed stating, "At least one digital certificate was found that matched your input". Read the terms of the subscriber agreement found on this page. If a message is displayed that no certificates were found that match the criteria chosen, click on the link **Try another search** and go back to step 7.
   NOTE: If there are other FBI NICS E-Check users at an FFL location that have the same name, the name that appears in the digital certificate will be appended with a number. For example, if there are two John Smith's, one will be identified as John Smith-1 (the first John Smith will be identified as John Smith). NICS Customer Service will notify the user when notification of the digital certificate is issued.
10. If the subscriber agreement is accepted, proceed to download the digital certificate by scrolling to the list of digital certificates found on the bottom of the page. Click on the **Download digital certificate** link next to your name Usually this list will have only a single entry, but

multiple digital certificates could be displayed.

11. The "Certificate Download" page will be displayed showing the contents of the digital certificate. Scroll to the bottom of this page and click the **Install Client Certificate** button.
12. Click the **Install** button on the next page that is displayed.
    NOTE: If the user attempts to download a digital certificate not belonging to that user, an error stating, "Unable to install the certificate" will appear. If this happens, go back and select a different link from the digital certificate list in step 9 or call NICS Customer Service.
13. A small window will be displayed stating "Your new certificate has been successfully installed!". Click the **OK** button.
14. Proceed to Section 6.3.4. Exporting a Digital Certificate—Step 5.

6.3.4 Exporting a Digital Certificate—Step 5

The digital certificate that was downloaded from FBI NICS E-Check can only be used on the browser that was used to download the digital certificate unless special procedures are followed. Once downloaded, the digital certificate can be copied to other computers or browsers for use. The process of copying a digital certificate from its usual location (inside the browser's database) to another location (i.e. floppy diskette, windows folder, etc.) is called exporting. The digital certificate can still be used from its original location after it has been exported. Exporting only generates a copy of the original digital certificate.

It is also a good idea to backup the digital certificate and its "private key" to a floppy diskette so that it may be recovered in the event of a computer failure. Backing up the digital certificate is accomplished through the exporting process.

To export a digital certificate:

1. Start Internet Explorer.
2. From the Menu Bar select **Tools, Internet Options…** to display the "Internet Options" window.
3. Select the **Content** tab, **Certificates…** to display the "Certificates" window.
4. Click the **Personal** tab.
5. Select your FBI NICS E-Check digital certificate then click the **Export…** button. This will display the "Welcome to the Certificate Export Wizard" window.
6. Click the **Next** button on the Certificate Export Wizard.
7. Choose **Yes, Export the Private Key** and click the **Next** button.
8. Remove the check marks from all boxes and click the **Next** button.
9. A window appears to "Create a password to protect this item". In the "Password for:" box, enter a name to identify your unique digital certificate (this could be your name) and **remember it**. In the "Password:" and "Confirm:" boxes, enter a password of your choosing (this could be the same password that was used in step 8 of Exporting a Digital Certificate) that will be used to protect your digital certificate and **remember it** (you will need this password every time you log into FBI NICS E-Check). Click the **Next** button.
   *NOTE: **Remember your password!** NICS Customer Service has no knowledge of user passwords. However, if a password is forgotten, contact NICS Customer Service for further instructions.*
10. Click the **Browse** button and choose the **3 ½ Floppy (A:)** from the pull down (Exporting to other locations such as your hard-drive, CD, Zip drive, etc. is possible). Enter a name for the

exported digital certificate "File name:" box. Proceed by clicking the **Save** button.

11. Click the Next button then the **Finish** button. Click **OK**. Highlight your FBI NICS E-Check digital certificate by selecting it then click Remove.
12. Click **Yes** and proceed to **Import Your Digital Certificate**.
13. Click **Close** and close the Browser.

6.3.5 Importing Your Digital Certificate

The process of copying a digital certificate into a browser from an exported file is called importing.

To import a digital certificate:

1. Start Internet Explorer if it is not already running.
2. From the Menu Bar select **Tools, Internet Options…** to display the "Internet Options" window.
3. Select the **Content** tab, **Certificates…** to display the "Certificates" window.
4. Click the **Personal** tab.
5. Click on the **Import…** button. The "Certificate Import Wizard" window is displayed.
6. Click the **Next** button.
7. Another "Certificate Import Wizard" window is displayed, prompting for a filename. Click the **Browse...** button.
8. From the "Open" window, choose the **3-½" floppy (A:)** (or other source that you may be importing from) on the "Look in:" drop down.
9. The digital certificate exported earlier should appear. Select the appropriate digital certificate and click the **Open** button.
10. The "Certificate Import Wizard" is again displayed. Click the **Next** button.
11. Another "Certificate Import Wizard" window is displayed prompting for the password that was used to protect the digital certificate when it was exported. Enter the password set in step 9 of Exporting a Digital Certificate.
12. Place check marks in both check boxes and click the **Next** button. Another Certificate Import Wizard" window is displayed concerning the "Certificate Store".
13. Select "Automatically select the certificate store based on the type of certificate" and Click the **Next** button.
14. The final "Certificate Import Wizard" window is displayed stating, "Completing the Certificate Import Wizard". Click the **Finish** button.
15. A "Importing a new private exchange key!" window is displayed. Click the **Set Security Level…** button.
16. Another "Importing a new private exchange key!" window appears. Choose the **High** security level option and click the **Next** button.
17. Another window is displayed prompting the user to create a new password that will be used to access the digital certificate.
18. Enter a password to encrypt the private key that is being exported. It will be necessary to enter this password in both the "Password:" and "Confirm:" boxes. Enter the chosen passwords and click the **Finish** button. (See Section 4.1.1)
    *NOTE: **Remember your password!** NICS Customer Service has no knowledge of user passwords. However, if a password is forgotten, contact NICS Customer Service for further instructions.*
19. Click the **OK** button on the "Importing a new private exchange key!" window that remains.

20. Click the **OK** button on the small confirmation window stating "The import was successful"
21. Click the **Close** button on the "Certificates" window that remains displayed in your browser.
22. Click the **OK** button on the "Internet Options" window.

6.3.6 Session Log on—Step 6

Each time a different user logins to FBI NICS E-Check from the same computer, Internet Explorer must be closed and re-started so the proper digital certificate can be presented to the FBI NICS E-Check Web site.

1. Connect to the Internet through an Internet Service Provider (if not already connected).
2. Start Internet Explorer (if not already running) and go to https://www.nicsezcheckfbi.gov/ (be sure to include the "s" in https). Depending on the browser's settings, a security alert may be displayed. If this occurs, click the **Yes** button on that window. The browser will display a "Client Authentication" window allowing the selection of a digital certificate when connecting.
3. Click on **Log on to NICS E-Check** link.
4. Highlight your digital certificate by clicking on it once, then click **OK**.
5. The "Signing Data with your Private Exchange Key!" window will appear prompting you to enter your digital certificate password. This is the password that was set in step 9 of ExportingYour Digital Certificate. Enter the password and click **OK**.
   NOTE: Do not select "Remember your password".
6. The FBI NICS E-Check Notice page will be displayed. Click **Continue**. The "Terms and Conditions" page appears. Read this carefully. To accept the terms and conditions, click the **AGREE** button, or click the **DISAGREE** button to exit.
7. The "FBI NICS E-Check Login" page will be displayed. Enter the appropriate FFL number, user codeword, username and phone number (including area code) and click the **Submit** button.
8. If login was successful, the "FBI NICS E-Check Search Request" page will be displayed. If login was unsuccessful, the login page appears where a retry is necessary.

6.3.7 Session Logoff

1. While logged in, click **EXIT** on top of any FBI NICS E-Check page. The "Terms and Conditions" page appears.
2. Close the Internet browser to ensure that no other individual may access your digital certificate.

6.3.8 Viewing a Digital Certificate

Once downloaded, the digital certificate and its content may be viewed at any time.

To view a digital certificate:

1. Select **Tools, Internet Options…** found in the menu bar of Internet Explorer. The "Internet Options" window will be displayed.
2. Select the **Content** tab from this window.
3. Click on the **Certificates…** button. The "Certificates" window will be displayed.

4. Select the **Personal** tab.
5. Select **All** in the "Intended purpose:" drop-down box.
6. Highlight the appropriate FBI NICS E-Check digital certificate by clicking on it once.
7. Click the **View** button to view the contents of the digital certificate.

6.3.9 Removing a Digital Certificate

It may become necessary to remove an FBI NICS E-Check digital certificate. This process is useful when an employee leaves an organization. The following procedure can be used to permanently remove an FBI NICS E-Check digital certificate.

To remove a digital certificate:

1. Start Internet Explorer if it is not already running.
2. From the Menu Bar select **Tools, Internet Options…** to display the "Internet Options" window.
3. Select the **Content** tab, **Certificates…** to display the "Certificates" window.
4. Click the **Personal** tab.
5. Select the digital certificate that is to be removed.
6. Click the **Remove** button.
7. A warning window will appear stating "You cannot decrypt encrypted data using the certificates. Do you want to delete the certificates?" Click the **Yes** button.
8. Click the **Close** button on the "Certificates" window.
9. Click the **OK** button on the "Internet Options" window.
10. Close the Browser.

6.3.10 Digital Certificate Expiration and Rekey Request

To further enhance the security of issued digital certificates, each digital certificate has an expiration date imposed upon it making it useful for a specified period of time. This time period is known as the validity period of the digital certificate. Typically, validity periods will range from 1 year to 18 months. Once a digital certificate has expired, it can no longer be used to obtain FBI NICS E-Check access. Thirty days prior to the end of the validity period, NICS Customer Service will contact the user. Upon notification, the user must submit an online digital certificate request and obtain a new certificate through the process outlined in section 6.3.2 above. It is not necessary, however, to submit another NICS/E-Check FFL Enrollment form unless the certificate has expired or been revoked.

To view your digital certificate's validity period:

1. Start Internet Explorer if it is not already running.
2. From the Menu Bar select **Tools, Internet Options…** to display the "Internet Options" window.
3. Select the **Content** tab, **Certificates…** to display the "Certificates" window.
4. Click the **Personal** tab.
5. Select **All** in the "Intended purpose:" drop-down box.
6. Highlight the appropriate FBI NICS E-Check digital certificate by clicking on it once.
7. Click the **View** button to view the contents of the digital certificate.

7 WINDOWS SPECIFIC PROCEDURES FOR USERS

7.1 Setting a Screen Saver Password

A Windows screen saver password should be set and configured to prevent someone from using a computer and possibly gaining access to personal digital certificates.

To set Windows screen saver password:

1. Use the left mouse button to click on the desktop and right click on **Properties**.
2. Select the **Screen Saver** tab to display the Screen Saver settings.
3. Select any screen saver in the drop down list except the one labeled "none".
4. Check the Password protected check box to enable password protection.
5. Set the Wait time to 15 minutes to ensure that the screen will be password protected after 15 minutes of inactivity.
6. Click the **OK** button.